UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/813,358	03/31/2004	Alan Frank Graves	14658	5013

293 7590 03/20/2008

Ralph A. Dowell of DOWELL & DOWELL P.C.
2111 Eisenhower Ave
Suite 406
Alexandria, VA 22314

EXAMINER	
POLTORAK, PIOTR	
ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
03/20/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/813,358	GRAVES ET AL.	
	Examiner	Art Unit	
	PETER POLTORAK	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12/07/07*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10,12-15,18-50 and 53-55* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *53-55* is/are allowed.

6)☒ Claim(s) *1-10,12-15,18-22 and 34-50* is/are rejected.

7)☒ Claim(s) *23-33* is/are objected to.

8)☒ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant amendment received on 12/07/07 have been entered.
2. Applicant amended claims 1, 15, 49 and 53-54. Claims 11, 16-17, 51-52 and 56-60 have been cancelled.

Response to Arguments

3. In light of applicant arguments and amendments the objections and 35 USC § 112 rejections cited in the previous Office Action are withdrawn.
4. *As per claim 15, applicant argues that Windows NT does not teach "a control entity of an end-user device being operative to apply a policy based on stimuli received via a user interface and a network interface in order to determine whether confidentiality of sensitive information stored in a memory store during a session for authentication user is to be preserved." To summarize applicant arguments, applicant suggests that functionality disclosed by Windows NT (e.g. Schmidt) is invoked "before a user is authenticated" thus not meeting the limitation of "a user interface for interfacing with the authenticated user".*

   Applicant arguments are not found persuasive. First, the examiner points out that a user interface such as keyboard (e.g. a user pressing keys "Cntrl+Alt+Delete" interfaces with computer systems) is an interface for a user (e.g. authenticated user) either before or after the authentication process. Secondly, claim 15 is a product claim and nothing in the claim language requires that the limitation "a user interface for interfacing with the authenticated user" must happen after the limitation "the control entity further operative to ....". Thirdly, an ordinary artisan would clearly

recognize that using "Cntrl+Alt+Delete" a user can "lock" Windows NT, so that no other user accesses the system during the authenticated user being away from his desktop. The unlocking process validates the authenticated user credential even though it is essentially similar to the regular log-on process (when a different user attempts to log on to the system as indicated by the message "This computer is being locked. Only *LoginNameUser* or an Administrator can unlock this computer".) Lastly, the limitation "a user interface *for interfacing with the authenticated user*" is a recitation directed to the manner in which a claimed apparatus is intended to be used does not distinguish the claimed apparatus from the prior art if prior art has the capability to do so perform (See MPEP 2114 and Ex Parte Masham, 2 USPQ2d 1647 (1987)). As clearly disclosed by Schmidt, Windows NT has capability to enable an authenticated user to interface with the server.

5. *As per applicant argument that that Widows NT functionality "in no way involves the end user device making a determination based on stimuli received via a network interface"* the examiner points out that an ordinary artisan would recognize that "Cntrl+Alt+Delete" sequence protect password by virtue of temporarily deactivating processes. Furthermore, successful/unsuccessful log on process (or unlock process), is based on stimuli from the user interface and a network interface) and determines whether confidentiality of sensitive information stored in a memory store during a session for authentication user is or is not to be preserved.
In regard to Blakley's and Schneier's references applicant repeats previously addressed arguments. However, it is not clear why applicant argues these

references, since there were not used in rejection of claim 15. As a result, Blakley's and Schneier's references will not be addressed in regard to applicant arguments directed towards claim 15.

6. *As per the rejection of claim 15 over Windows NT/2000 rejection applicant presumably argues an ordinarily skilled person looking at the cited art would be led to the claimed end user device, which comprises a control unit operative to apply a policy based on stimuli received via its user interface and network interface supporting the position by suggesting that "it is a user, and thus not his/her end user device.*

   Applicant arguments are not quite understood. An ordinary artisan would readily recognize that although a user works with his device (an end user device) in order for a particular activity to be accomplished (i.e. preserving confidentiality of the sensitive information stored in the memory store), ultimately an element in the end user device's, which must detect, interpret/determine and respond accordingly to received stimuli must be present. This element reads on the control entity recited in the claim language.

   Additionally, the examiner points out that the limitation requires only the end user device to be operative (or in other words, to have capability) to performed limitations of claim 15, which end user devices such as computer running Windows NT/2000 inherently have.

7. *As per newly amended claim 49, applicant appears to argue already addressed claimed limitations.* Thus, the examiner refers applicant to response above.

8. *As per claim 1 applicant argues that neither Blakley, Schneier and White nor Fairclough teach "a selection module that allows data to be selectively exchange either with an encryption module or directly with a memory store, bypassing the encryption module". Applicant argues that "object 15" in Blakley's Figure 1 refers to a "daemon and APIs" executing on a host server that requests cryptographic operations to be performed by Blakley's cryptographic accelerator. Thus, applicant suggests that object 15 is used to perform cryptographic operations and do not allow data to be exchanged directly in a memory without being encrypted/decrypted".*

It appears that applicant attempts to argue limitation most similar to previously presented claim 11 and now incorporated into claim 1. This claim was rejected over White in view of Fairclough. Thus, it is not clear why applicant argues Schneier references that were not used in rejection of claim 11. As a result, applicant arguments regarding these references will not be addressed.

In order to address applicant arguments directed towards claim 15, the examiner notes a typographical error: it is an object 2 and not 15 that was been considered to represent the selection module.

Furthermore, the examiner points out that "bypassing the encryption module" is not present in the claim limitations. However, the limitations of claim 15 are clearly taught by White in view of Fairclough. The examiner points out that the limitation "the selection module being capable of ..." is a recitation directed to the manner in which a claimed apparatus (i.e. a selection module of a data processing apparatus) intended to be used does not distinguish the claimed apparatus from the prior art if

prior art has the capability to do so perform (See MPEP 2114 and Ex Parte Masham, 2 USPQ2d 1647 (1987)). As clearly shown in Fig. 1 and recited in col. 3 lines 41-67, object 2 utilizes daemon and APIs executed in a user device. An ordinary artisan would readily recognize that not only daemon and APIs executing on a user device are capable but in fact they inherently access a memory store of the user device. Thus, the selection module (object 2) is capable to exchange data directly with the memory store. The examiner also points out that in situation wherein an encryption is selected, the data from end user device taught by Fairclough must go through the selection module, in order to exchange data with the encryption module disclosed in Fig. 1. Thus, contrary to applicant assessment, White in view of Fairclough clearly teach the selection module capable of selectively exchange data either with an encryption module or directly with a memory store.

9. As per claims 53-55, applicant points out that the claims have been rewritten in independent form to incorporate the limitation that were not found in the prior art.

10. Claims 1-10, 12-15, 18-50 and 53-55 have been examined.

11. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 102 or 103

12. Claims 15, 18-22, 34, 36-37, 49-50 remain rejected under 35 U.S.C. 102(b) as anticipated by or, in the alternative, under 35 U.S.C. 103(a) as obvious over

Windows NT/2000 as illustrated by Schmidt (Jeff Schmidt, "Microsoft Windows 2000 Security Handbook", ISBN: 0789719991, August 2000).

As per claims 15-22, 34, 49 Schmidt teaches Window NT/2000 network environment implementing an end user device communicating with a server (e.g. Fig. 13.1, pg. 268). Schmidt discloses server supporting for authenticated users (e.g. "Authentication", pg. 277), and discloses that the system supports TCP/IP communication (pg. 147). In TCP/IP each communicating entity manages a communication session (e.g. "Large Window Support", pg. 147). Furthermore, an ordinary artisan would recognize that computers utilizing Windows NT/2000 comprise a memory store (e.g. hard disks) and are operative to store sensitive information (e.g. SAM database, pg. 318) during the session.

13. Schmidt discloses that end user device determine whether confidentiality of the sensitive information stored in the memory store is to be preserved and responsive to determining the confidentiality of the sensitive information stored in the memory store is to be preserved, taking an action to preserve confidentiality of the sensitive information stored in the memory store based on stimuli received via the user interface and the network interface ("The General Logon Sequence" and "Authentication Procedure", pg. 320-322, and "Account Lockout Policy", pg. 560, for example. Note that Windows provides at least two types of procedures that read on the claim language. In addition to prevent a user to access confidential information when input password and user name do not are not correct Windows protects

confidential information responsive to Control-Alt-Delete command, see USPN 5664099 referring to Windows NT, for example).

14. The examiner considers Microsoft 2000, Kernel to read on the control entity.

15. As per newly introduced limitations, the examiner points out that end user devices utilizing Windows NT/2000 comprise a user interface for interfacing with the authentication user (e.g. keyboard) and a network interface for interfacing with the server (e.g. contacting a Domain Controller in order to validate user's credentials or accessing a file server to store retrieve information) and the control entity operative to apply a policy based on stimuli received via the user interface and the network interface (for more details see the discussion in Response to Agreements section, above).

16. As per claim 34, only a proper authentication allows a user to pass the log-in module and access the memory store.

17. As per claim 36, Schmidt discloses Microsoft 2000's Encrypted File System (EFS, 210 and 470-471).

18. As per claims 37, Microsoft 2000 locking an account suggested by Schmidt on pg. 560 would result in disabling a user interface.

19. As per claim 50, Schmidt does not disclose that the sensitive information comprises healthcare information. However, the examiner points out that giving a particular name to the information (e.g. healthcare information) would not affect the functionality of Schmidt's invention, in particular the claimed end user device cited in the claim language 15. Furthermore, Schmidt does not offer any restriction

regarding the user of the end user device and an ordinary artisan in the art of healthcare would readily recognize that any information in healthcare environment (healthcare information) could be considered sensitive. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include Schmidt invention to operate in healthcare environment and thus comprise healthcare information given the benefit of additional security. See, KSR ruling. Additionally, the Official Notice is taken that it is old and well known to store sensitive information that is healthcare information in a memory store (e.g. medical records stored on PCs and/or Servers, e.g. USPub. 2002/0026105, USPub. 2003/0179223, USPub. 2003/0208382 etc.), and it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to implement Microsoft 2000 invention as disclosed by Schmidt into healthcare information given the benefit of security.

20. Claims 15, 35-36, 44-50 remain rejected under 35 U.S.C. 102(b) as anticipated by or, in the alternative, under 35 U.S.C. 103(a) as obvious over Windows 2000 as illustrated by Microsoft TechNet" (Microsoft TechnNet "Data Protection Implementing the Encrypting File System in Windows 2000" posted in "Windows 2000 File Systems Tutorials", in particular: "Step-by-Step Guide to Encrypting File System (EFS)" article on 05/2002).

As per claims 15, 49-50, Microsoft TechNet discloses encrypting a file or folders by Windows 2000 ("Encrypting a file or folder"). End user devices implementing Windows 2000 are implemented on computers and computers comprise processor and memory. The process of encrypting files or folders evidences the presence of a

memory store operative to store sensitive information during the session. Windows 2000 discloses that determining whether confidentiality of the sensitive information stored in the memory store is to be preserved and responsive to determining that confidentiality of the sensitive information store in the memory store is to be preserved, taking an action to preserver confidentiality of the sensitive information stored in the memory store (see "Encrypt contents to secure data selection" in "Encrypting a file or folder" section).

21. As per newly introduced limitations, the examiner points out that end user devices utilizing Windows NT/2000 comprise a user interface for interfacing with the authentication user (e.g. keyboard) and a network interface for interfacing with the server (e.g. accessing a file server to encrypt stored/sensitive information) and the control entity operative to apply a policy based on stimuli received via the user interface and the network interface (an element in the end user device determining files/folders on a remote server that are communicated to the user and selected to be encrypted).

The "Folder and File Encryption on a Remote Server) provides evidence of a control entity operative to support a session with the server for an authenticated user. Furthermore, the decryption process disclosed in "Decrypting Files and Folders" section reads on claim 44 and as per claim 45, Windows 2000 discloses that in order to provide encryption an authorized administrator must enable encryption ("Encrypting a file or folder" section) and an ordinary artisan would readily recognize that in addition to a user interface enabling encryption in order to encrypt files on a

remote server (as disclosed in "Folder and File Encryption On a Remote Server" section) requires a network interface.

22. As per claim 36, encryption reads on data scrambling.

23. As per claim 35, an ordinary artisan would readily recognize that encryption would replace the unencrypted information and, as a result, the sensitive (unencrypted information) would be erased.

24. As per claim 47, although Windows 2000 does not disclose that the end user device is a mobile wireless device, an Official Notice is taken that it is old and well known in the art of computing to use mobile wireless devices (e.g. laptops in wireless Ethernet environment), and it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to implement Windows 2000 invention in an end user device that is a mobile wireless device given the benefit of portability.

25. As per claim 48, a wireless interface/card provides information regarding the interface (e.g. 802.11 standard connection), which would read on a label, and since each interface has different maximum distance from a receiver the examiner treats the label broadly as indicative of an inability to function outside a predetermined location.

Also, the examiner points out that any distance outside of a predetermined network location result in no network connection and mobile devices frequently disclose indication that there is no network connection (see Thurrott, for example). This display also reads on the label.

26. Additionally, although Windows 2000 do not explicitly disclose that the sensitive information comprises healthcare information, the examiner points out that giving a particular name to the information (e.g. healthcare information) would not affect the functionality of Windows 2000 invention, in particular the claimed end user device cited in the claim language 15. Furthermore, Schmidt does not offer any restriction regarding the user of the end user device and an ordinary artisan in the art of healthcare would readily recognize that any information in healthcare environment (healthcare information) could be considered sensitive. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include Schmidt invention to operate in healthcare environment and thus comprise healthcare information given the benefit of additional security. See, KSR ruling. Additionally, the Official Notice is taken that it is old and well known to store sensitive information that is healthcare information in a memory store (e.g. medical records stored on PCs and/or Servers, e.g. USPub. 2002/0026105, USPub. 2003/0179223, USPub. 2003/0208382 etc.), and it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to implement Microsoft 2000 invention as disclosed by Schmidt into healthcare information given the benefit of security.

27. Claim 38-43 remain rejected under 35 U.S.C. 103(a) as obvious over Windows 2000 as illustrated by Microsoft TechNet" (Microsoft TechnNet "Data Protection Implementing the Encrypting File System in Windows 2000" posted in "Windows 2000 File Systems Tutorials", in particular: "Step-by-Step Guide to Encrypting File System (EFS)" article on 05/2002) in view of Blakley (USPN 5677952) and Schneier

(Bruce Schneier, "Applied Cryptography, Protocols, Algorithms and Source Code in C", 2nd edition, 1996 ISBN: 0471128457).

As per claim 38, Windows 2000 as illustrated by Microsoft TechNet discloses the end user implementing encryption in order to preserve confidentiality of the sensitive information stored in the memory store as discussed above.

28. TechNet is silent regarding details of the device. Specifically, TechNet does not disclose that the end user device implementing Windows 2000 comprises a data bus connected to the memory store, the data bus being adapted for transporting data to and from the memory store; an encryption module communicatively coupled to the control entity and to the data bus; the control entity being further operative to release read and write commands towards the memory store, the write command being accompanied by first data intended to be written to the memory store; upon the control entity releasing a write command accompanied by said first data, the encryption module being operative to encrypt, in accordance with an encryption key, said first data and send an encrypted version of said first data onto the data bus for writing into the memory store; upon the control entity releasing a read command, the encryption module being operative to decrypt, in accordance with a decryption key, an encrypted version of second data received from the memory store via the data bus and provide said second data to the control entity.

However, these details are disclosed by Blakley in view of Schneier's end user device implementing encryption/decryption, as discussed above. Both of these inventions are concerned with preserving confidentiality of information and both of

these inventions use encryption processes to facilitate the confidentiality. Thus, the advantages of the systems of Blakley in view of Schneier and TechNet could have been easily combinable with more than reasonable expectations of success. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to implement Blakley in view of Schneier's invention into TechNet invention in order to facilitate the process of information encryption.

29. The limitations of claims 39 and 41 are implicit. End user devices are not limited to a particular user. Thus, an encryption key (as well as corresponding decryption key) would have to be changed in order to ensure true confidentiality. Similarly implicit is limitation of claim 40. Leaving (not deleting) a decryption key violate the principle of data confidentiality because the retrieved decryption key would allow any party to compromise confidentiality of the encrypted information.

30. As per claims 42-43, "the previous decryption key" used prior to use of "the new decryption key" must be stored in memory at the time that process of encryption is taking place in order for the end user device being able to operate on it (the previous decryption key). Similarly, the decryption process (when confidentiality of the sensitive information no longer needs to be preserved) involves (previous) decryption key.

31. Claims 1-10 and 12-14 are rejected under 35 U.S.C. 103(a) as obvious over White (Ron White, "How Computer Work", 7th edition, ISBN: 0789730332, October 2003) in view of Fairclough (USPN 6963979).

As per claims 1, 8-9, White discloses that computer system comprise data bus system enable to communicate data between system's component (pg. 16-17 and 28-29, for example). The system comprises processing entity operative to release read and write commands (CPU, pg. 18, for example) to read write data in a memory store (e.g. Hard Drive, pg. 28 and 29, RAM pg. 17 etc.).

32. White does not disclose an encryption module being operative to encrypt/decrypt data written/read to/from the memory store.

Fairclough discloses an encryption module being operative to encrypt/decrypt data written/read to/from the memory store (e.g. Fig. 1 and col. 2 line 8- col. 3 line 25). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to implement an encryption module as disclosed by Fairclough given the benefit of data security.

The examiner considers object 2, in Fig. 1 to read on selection/control module, and as it is clear from Fig. 1, any cryptographic data (keys) handled by the encryption module is received from the selection/control module, and a signal received by the selection/control module indicates the need to exchange data (an encryption state) with the encryption module (for details, see the response to Applicant Arguments, above).

33. As per claims 2-6, 10 and 12-14, Fairclough discloses implementation of a common application-specific integrated circuit (ASIC, col. 4 lines 48-49), memory storing encryption and decryption key (Fig. 1, key storage) and use of symmetric keys (col. 4 lines 35-37). Although, Faricough does not explicitly disclose that the memory

storing keys is a volatile memory, col. 1 lines 43-55, for example, clearly discloses that implementation of a volatile memory would have been an obvious variation given the benefit of enable key exchange. Erasing the portion of the volatile memory upon receiving a signal indicating that the key is no longer needed, is implicit: an ordinary artisan in the art of computer security would readily recognize that keeping no longer used keys pose unnecessary security threats.

As per claim 7, although Fairclough suggests exchange of encryption keys (col. 1 lines 43-55), Fariclough's disclosure is silent regarding a policy applied in response to stimuli received from a host entity and a user of the data processing apparatus. However, an ordinary artisan would recognize the use of a program/software routine necessary to implement the process of exchange encryption keys. The examiner considers a particular implementation of use of the particular encryption keys (due to communication with a host entity and action of a user of the data processing apparatus) to read on a policy.

Conclusion

Claims 53-55 overcome the art of record.

Claims 23-33 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571) 272-3840. The examiner can normally be reached Monday through Thursday from 9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m.

/Peter Poltorak/

Examiner, Art Unit 2134

/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2134